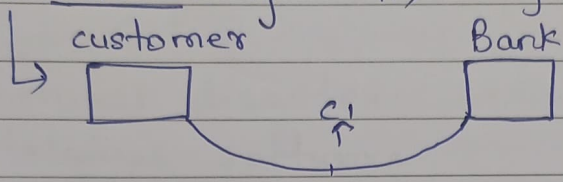
- GOAL OF SECURITY: (CIA)

i) Confidentiality. ii) Integrity iii) Availability.



{credit/ debit card

{Bank details

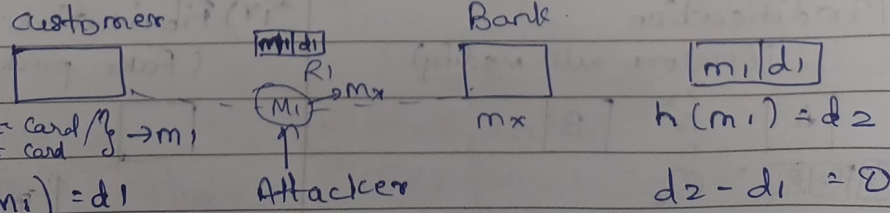
$E(M_1)_{K_1} = C_1$ (x) Attacker

Objective is to protect the information at sender and receiver side.

- Cryptography:
  - Encryption
    - Symmetric Encryption (same key is used for encryption as well as decryption)
    - Asymmetric Encryption (different keys are used for encryption as well as for decryption)

ii) Integrity:

Protecting or verifying the information in a communication channel in a intact format.



$\overset{M_1}{E(M_1)_{K_1}} = C_1 \longrightarrow$ Confidentiality.

$h(M_1) = d_1 \longrightarrow$ Integrity

$[C_1 :: d_1]$

$D(C_1) = M_1$

$h(M_1) = d_2$

$d_2 - d_1 = 0$

Drawback is if message (m_1) is modified as well as (d_i) is modified then there is no option

iii) Availability:

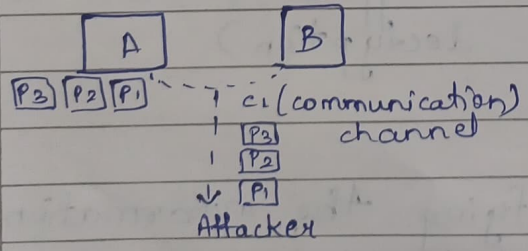
Accessibile to legitimate users only.

Access Control Matrix or Access control list.

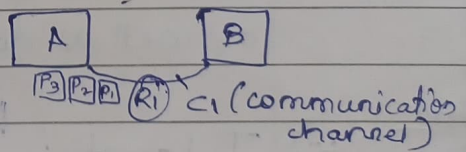
- Threats: weakness in a system.

Threats → Vulnerability → Attack → Protection

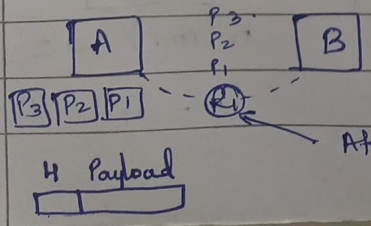
i) Interception.



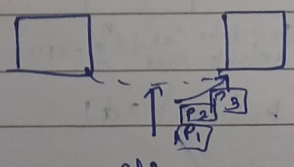
ii) Interruption Blocked



iii) Modification (Someone will modify)



iv) Fibrication. (Fake packets are generated)



__/__/____

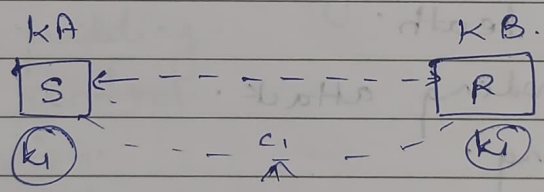
- **System Threats :**

i) Innocent persons.
ii) Scripts kiddies.
iii) Hackers / crackers.
iv) Insider persons.
v) Nation.
vi) Natural disaster.
vii) Malicious software.

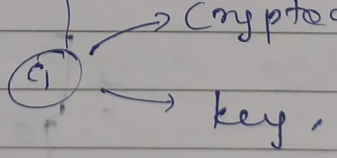
- **Security Vulnerability :**

i) Lack of strong password.
ii) Lack of malware removal tool.
iii) Poor access control.
iv) Unpatch software.
v) Device misconfiguration.

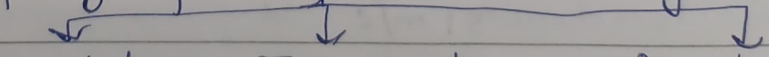
- Cryptographic Attack - key.



Credit info.



- Non-cryptographic attack - Security attack



Confidentiality Attack
@ Snooping.
⑥ Trafic analysis.

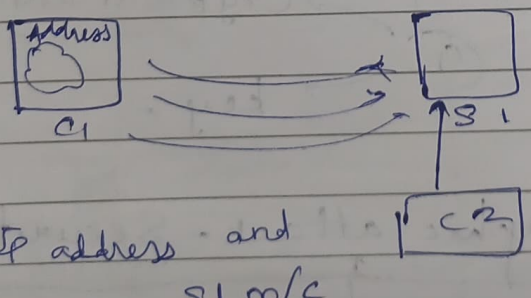
Integrity Attack
@ Modification
⑥ Mas querating.
© Replay.
ⓓ Repudation.

Availability attack

Types of Attack:-

i) Cryptographic Attack:
In this attack attacker need to obtain the secret key which is used for encryption and decryption operation.

ii) Non-cryptographic Attack:
- Confidentiality Attacks:
  (a) Snooping
  (b) Traffic analysis.
- Integrity attack
  (a) Modification
  (b) Masquerading
  (c) Replay.
  (d) Repudation.
- Availability Attack:
  (a) DoS
  ~~DOS can be catagorized into:~~
  - Intentional DOS attack
  - Non-intentional DOS attack. - (Amazon offer)
  (1) Ping and death.
  (2) SYN - flooding attack.
  (3) IP spoofing.



> ping IP address and
S1 m/c

__/__/__

- **Security Services:**

i) Data confidentiality.
Solution: Cryptography / Hashing.

ii) Data integrity.
Solution: Hashing, Anti change, Anti-replay.

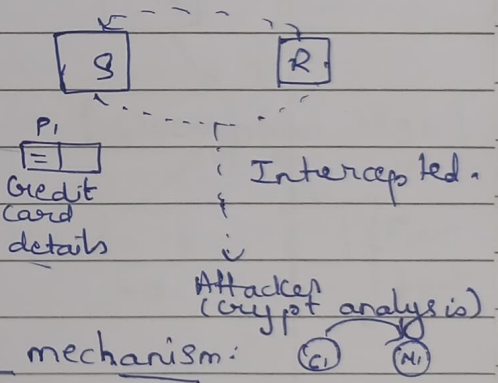
iii) Authentication.
Solution: Peer entity, data origin authentication.
(TCP) connection oriented → connection less (UDP).

iv) Non-Repudation.
Solution: Proof of origin → digital signature, Proof of delivery → protocol.

v) Access control.
Solution: ACL / ACM

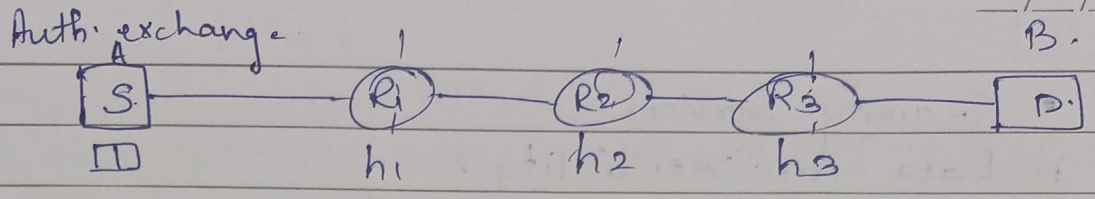
- **Security Mechanism:**

i) Encipherment.
ii) Data integrity.
iii) Authentication exchange.
iv) Traffic padding.
v) Routing control.
vi) Notarization.
vii) Access control.



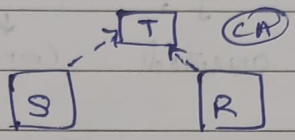
- **Relation between Services and mechanism:**

Security Services	Security mechanisms
i) Data confidentiality.	Encipherment and Routing controls.
ii) Data Integrity.	Encipherment, Digital signature, hashing.
iii) Authentication	Encipherment, Digital Signature, Auth. exchange.



iv) Non-Repudation — Digital signature, Data Integrity (Hash), Notarization.

Notarization:



v) Access control | Access Control Mechanism

- Cryptography:

Stream cipher Block cipher

Encryption

input text → abcdefgh (x) Plain text (P_x) → Cipher text (x)

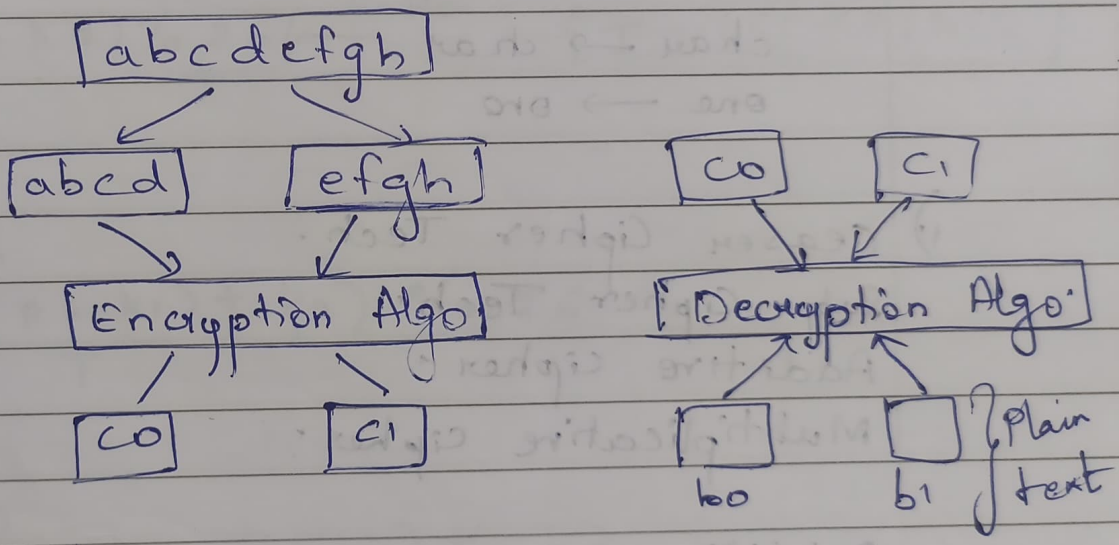
↓ a

Encryption Algo. Decryption Algo.

Cipher Text → C_1 Plain text (P_x)

C_x

Block cipher:



1. Stream cipher Tech:

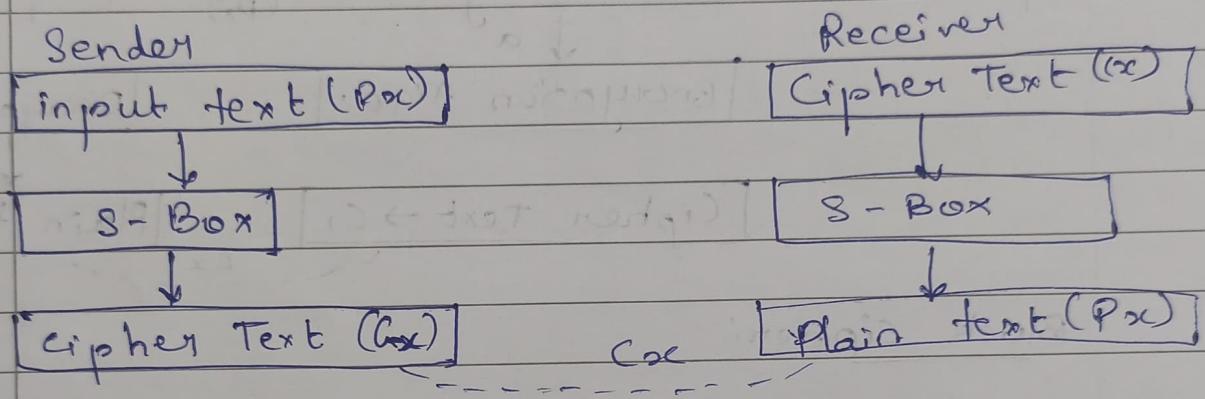
i) Substitution Tech. ii) Transposition Tech.

a	b	c	d		...
t	m	k	x		

S-Box

Sender ↔ Receiver

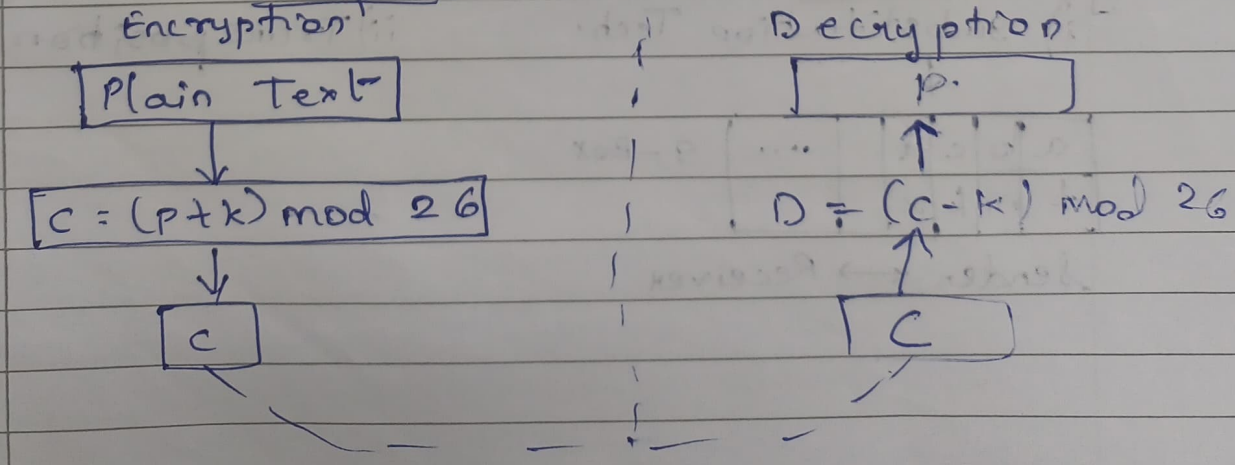
1) Monoalphabetic Ceaser Cipher Technique:
In this, each character is replaced by its another character by using substitution table. Substitution table should be mutually agreed by sender and receiver. Another approach, sender can generated the substitution table which he will share with receiver.



char → char
one → one

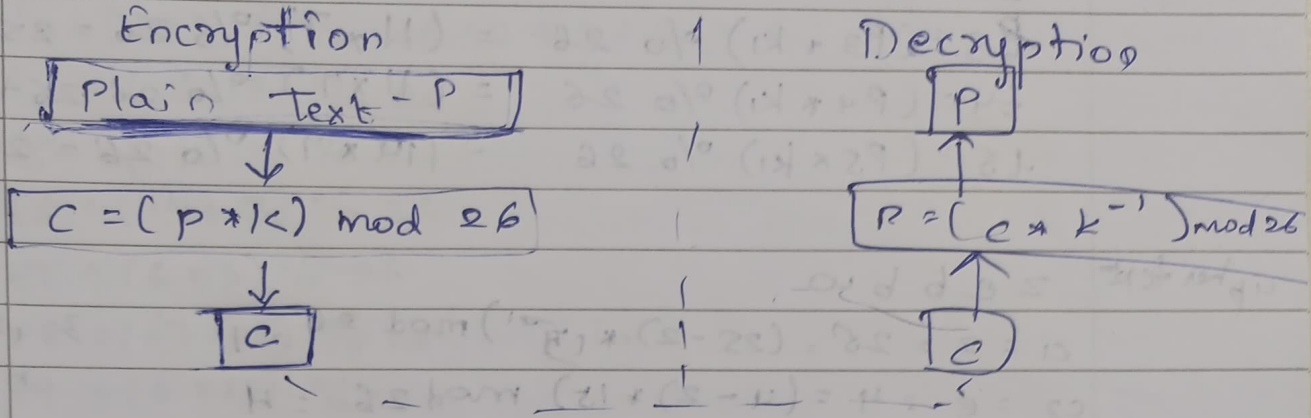
1) Ceaser Cipher Tech.
Sub. Cipher Tech.
Additive cipher
Multiplicative cipher.

- Additive Cipher Tech.

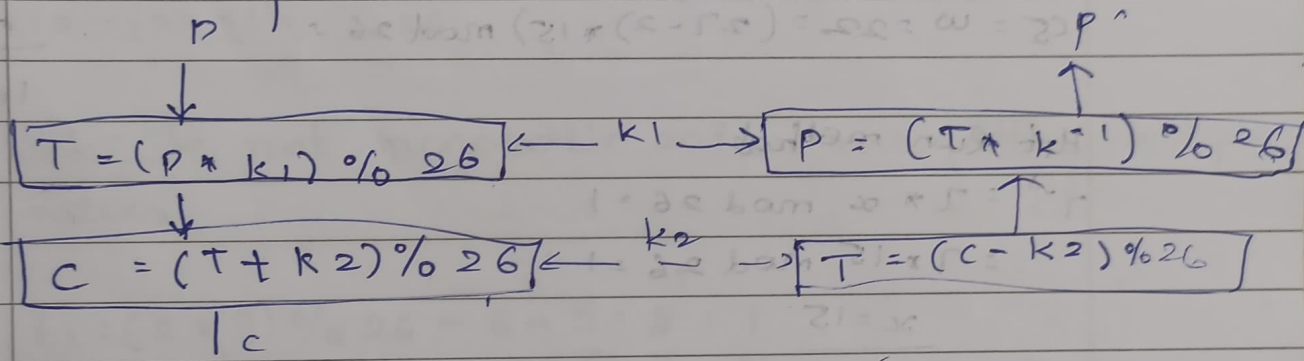


__/__/__

- **Multiplicative Cipher Tech:**



- **Affine Cipher Tech:**



Encryption

$C = ((P * K_1) + K_2) \% 26$

T

Decryption

$P = ((C - K_2) * K^{-1}) \% 26$

T

Q. Encrypt "hello" using affine cipher Tech.
key (7, 2) = (K_1, K_2)

→ 1) p1 p2 p3 p4 p5
h e l l o
7 4 11 11 14 → index value

a → 0
:
z → 25

$t_1 = (P_1 * k_1) \% 26 = (7*7) \% 26 = 23 + 2 = 25 = z$

$t_2 = (P_2 * k_1) \% 26 = (4*7) \% 26 = 2 + 2 = 4 = e$

$t_3 = (P_3 * k_1) \% 26 = (11*7) \% 26 = 25 + 2 = 27 \% 26 = 1 = b$

$t_4 = (P_4 * k_1) \% 26 = (11*7) \% 26 = 25 + 2 = 27 \% 26 = 1 = b$

$t_5 = (P_5 * k_1) \% 26 = (14*7) \% 26 = 20 + 2 = 22 = w$

Ciphertext: z e b b w

$c_1 = z = 25 = (25-2) * 15^{-1}) \bmod 26 = 1$

$c_2 = e = 4 = (4-2) * 15) \bmod 26 = H$

$c_3 = b = 27 = (27-2) * 15) \bmod 26 =$

$c_4 = b = 27 = (27-2) * 15) \bmod 26 =$

$c_5 = w = 22 = (27-2) * 15) \bmod 26 =$

3 15
7
5

2 26
4
10 4

Hit Run method

$7^{-1} = 7 * x \bmod 26 = 1$

$= 7 * 15 \bmod 26 = 1$

$x = 15$

1 26
3
7 3

Another method 7^{-1}

$(26 * x + 1) / 7 = 1$

$(26 * 1 + 1) / 7 =$

$(26 * 2 + 1) / 7 =$

$(26 * 3 + 1) / 7$

$(26 * 4 + 1) / 7 =$ (15)

Perform encryption and decryption operation using affine tech. for following plain text "cryptography" key = (*3, *5)

Note:

1) $gcd(k_1, 26) = 1$ (k1)
2) $1 \le k_1 \le 25$
3) $0 \le k_2 \le 25$

} To generate key 3 conditions should be matched (k2)

	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12
	c	r	y	p	t	o	g	r	a	p	h	y
	2	17	24	15	19	14	6	17	0	15	7	24

a - 0
b - 1
c 2
d 3
e 4
f 5
g 6
h 7
i 8
j 9
k 10
l 11
m 12
n 13
o 14
p 15
q 16
r 17
s 18
t 19
u 20
v 21
w 22
x 23
y 24
z 25

t1 = (2 * 13) % 26 = 0 + 2 = 2 = c.

t2 = (17 * 13) % 26 = 13 + 2 = 15 = p.

t3 = (24 * 13) % 26 = 0 + 2 = 2 = c

t4 = (15 * 13) % 26

t5 = (19 * 13) % 26

t6 = (14 * 13) % 26

t7 = (6 * 13) % 26

t8 = (17 * 13) % 26

t9 = (0 * 13) % 26

t10 = (15 * 13) % 26

t11 = (7 * 13) % 26

t12 = (24 * 13) % 26

Note: Its not monolathic and we are getting multiple values

t1 = (2 * 3) % 26 = 6 + 5 = 11 = l

t2 = (17 * 3) % 26 = 25 + 5 = 30 % 26 = 4 = e.

t3 = (24 * 3) % 26 = 20 + 5 = 25 % = z

t4 = (15 * 3) % 26 = 19 + 5 = 24 = y

t5 = (19 * 3) % 26 = 5 + 5 = 10 = k

t6 = (14 * 3) % 26 = 16 + 5 = 21 = v

t7 = (6 * 3) % 26 = 18 + 5 = 23 = x

t8 = (17 * 3) % 26 = 25 + 5 = 30 % 26 = 4 = e

t9 = (0 * 3) % 26 = 0 + 5 = 5 = f

t10 = (15 * 3) % 26 = 19 + 5 =

t11 = (7 * 3) % 26 =

t12 = (24 * 13) % 26 =

l
e
z
y
k
v
x
e
f
y
a
z

- **Playfair cipher Technique.**
  - Symmetric Encryption Tech.
  - 625.

(1) Formation 5x5 matrix

Key: "moon mission".

5x5 = 25

(i j)

	1	2	3	4	5
1	m	o	n	i/j	s
2	a	b	c	d	e
3	f	g	h	k	l
4	p	q	r	t	u
5	v	w	x	y	z

(2) From given plaintext remove punctuation, special character and number.

(3) Make a pair of alphabets if last single character is remained then add 'x' value with the character

Ex: djsanghvi

dj sa ng hv i(x) → Added

(4) If any pair have same alphabet then stuff 'x' character in between them.

Ex: ab cc

↓ → stuffed character

ab cxc

Ex: Use playfair cipher tech. to encrypt plaintext "greet" using key "moon mission".

Ans. (2) greet

gr ex et

↓ ↓ ↓

hq cz du

Cipher tech: hqczdu

on → ni ds → jm hr → rx ty → yi

Use playfair cipher Tech. to encrypt the plaintext text = "why, don't you". using key = "keyword".

5×5 = 25

	1	2	3	4	5
1	k	e	y	w	o
2	r	d	a	b	c
3	f	g	h	i/j	l
4	m	n	p	q	s
5	t	u	v	x	z

wh yd on ty ou

yi ea es vk ez

- Hill cipher:
  - 1929
  - Poly alphabetic cipher Tech.
  - Matrix

char	value
a	0
b	1
.	.
.	.
.	.
z	25

OR

Find out index value of char.

Encryption : $C = (k * p) \bmod 26$.

Decryption : $p = (k^{-1} * c) \bmod 26$.

* Encrypt the message "exam" using Hill cipher Tech with key = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

Note: key should be always a square matrix.

Soln: p = exam

$k = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ key = 2×2 key = 3×3.

$p = \begin{bmatrix} e \\ x \end{bmatrix} = \begin{bmatrix} 4 \\ 23 \end{bmatrix}$

$\begin{bmatrix} a \\ m \end{bmatrix} = \begin{bmatrix} 0 \\ 12 \end{bmatrix}$

OR

Encryption: $c = k * p \bmod 26$.

(1) $= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 4 \\ 23 \end{bmatrix}$

$= \begin{bmatrix} 128 \\ 181 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 24 \\ 25 \end{bmatrix}$

(2) $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 0 \\ 12 \end{bmatrix}$

$= \begin{bmatrix} 48 \\ 84 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 22 \\ 6 \end{bmatrix}$

$\begin{bmatrix} 24 & 22 \\ 25 & 6 \end{bmatrix} = \begin{bmatrix} y & w \\ z & g \end{bmatrix}$

$c = yzwg$.

Encrypt message "DEF" using hill cipher Teh. with key: $\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 8 & 8 & 7 \end{bmatrix}$.

Soln:

$p = DEF$

$K = \begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 8 & 8 & 7 \end{bmatrix}$

$p = \begin{bmatrix} D \\ E \\ F \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix}$.

mod = remainder

__/__/____

$c = k * p \bmod 26$.

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 8 & 8 & 7 \end{bmatrix} * \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix}$$

$$= \begin{bmatrix} 47 \\ 40 \\ 91 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 21 \\ 14 \\ 13 \end{bmatrix}.$$

$$\begin{bmatrix} 21 \\ 14 \\ 13 \end{bmatrix} = \begin{bmatrix} V \\ O \\ N \end{bmatrix} \quad C = VON$$

* Convert following plaintext in ciphertext using key $\begin{bmatrix} 23 \\ 36 \end{bmatrix}$. Also perform decryption operation.

Soln: p : "ATTACK"

$$k = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$

$$p = \begin{bmatrix} A & T \\ T & A \end{bmatrix} \quad C = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$$

$$= \begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$$

$c = k * p \bmod 26$

$$\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} * \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} * \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 23 \\ 36 \end{bmatrix} * \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} 34 \\ 66 \end{bmatrix} \xrightarrow{\text{mod } 26} \begin{bmatrix} 8 \\ 14 \end{bmatrix}$$

C = IKNFIO.

Decryption.

$P = K^{-1} * C \bmod 26$.

$$K^{-1} = \frac{1}{|K|} * \text{adj}(K)$$

det^n. 2×2 matrix

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = |a \times d - b \times c|$$

$$\begin{bmatrix} 23 \\ 36 \end{bmatrix} = [12 - 9] = 3.$$

Multi. Inverse of determinant

$d * d^{-1} = 1 \bmod 26$.

$(3 * d^{-1}) \bmod 26 = 1$

$d^{-1} = 1$ ↳ Hit and run.

$d^{-1} = 9$

$(3 * 9) \bmod 26 = 1$ ✓

$d^{-1} = 9$

adj (K)

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & b \\ c & a \end{bmatrix} \Rightarrow \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= \begin{bmatrix} 23 \\ 36 \end{bmatrix} = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 6 & -3+26 \\ -3+26 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

__/__/____

$$K^{-1} = 9 * \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} * \begin{bmatrix} 5 & 12 & 8 \\ 10 & 5 & 14 \end{bmatrix} \text{ mod } 26.$$

$$\begin{bmatrix} 260 & 154 & 366 \\ 305 & 390 & 452 \end{bmatrix} \text{ mod } 26,$$

$$\begin{bmatrix} 0 & 19 & 2 \\ 19 & 0 & 10 \end{bmatrix}$$

P = ATTACK

- Vigenere Cipher Tech.

Encryption

$C_i = (P_i + k_i) \text{ mod } 26$

Decryption

$P_i = (C_i - k_i) \text{ mod } 26$

Ex: input P_i = a b c d (0, 1, 2, 3)

$k_i = 4532$

Cipher text (C_i) = (index value + k_0) + ... (index value + k_n)

Cipher text $(C_i) = (0+4) + (1+5) + (2+3) + (3+2)$

$= 4 + 6 + 5 + 5$

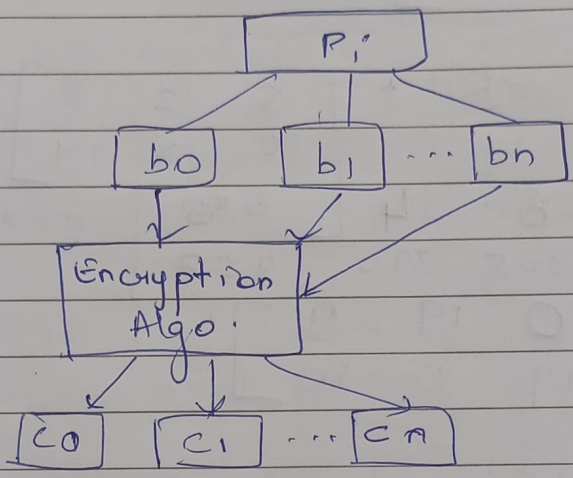
$=$ e g f f

Decryption:

(4-4) (6-5) (5-3) (5-2)

= 0 1 2 3

- Block Cipher Tech.

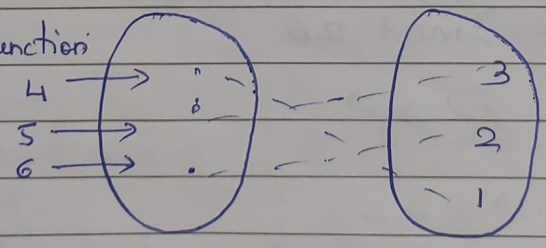


- Feistel Cipher Tech.

Feistel cipher Tech. has three functions or components.

i) Self invertible.
ii) Invertible.
iii) Non-invertible.
iv) Mixer.
v) Swapper.

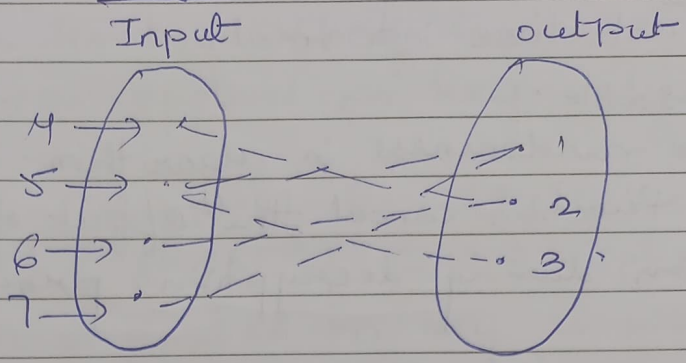
* Invertible function



one to one

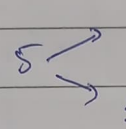
(456) → (132)

* Non-invertible function:



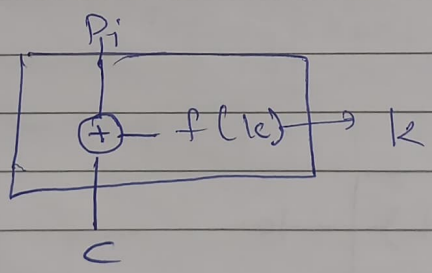
One to many

4 → 2
5 → 1
5 → 3
6 → 2
7 → 1

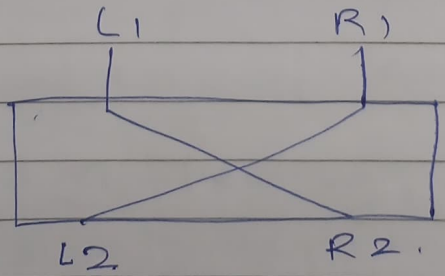


* Self-Invertible:
If function is equal to its inverse is called as self-invertible. i.e. $a == a^{-1}$

* Mixer:



* Swapper:

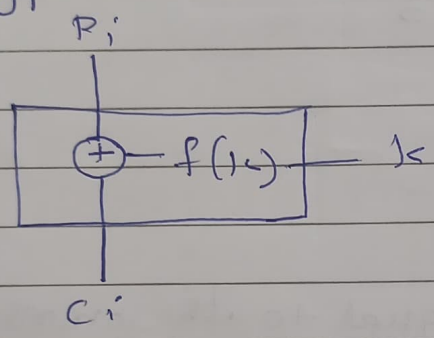


Why X-OR is used?

1. Does not lose information.
2. Reversable.
3. Induce randomness in algorithm.
4. X-OR function cancel the effect of encryption operation during decryption process.

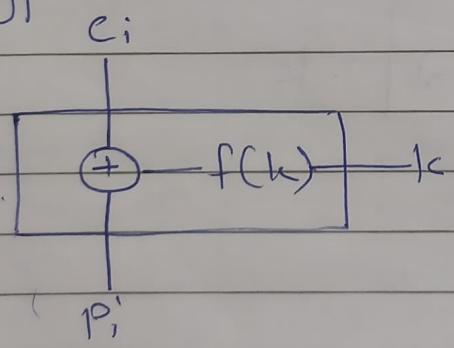
First Draft of Feistel Cipher Tech:

Encryption



$C_i = P_i \oplus f(k)$

Decryption



$P_i = C_i \oplus f(k)$

Ex: p=0111

f(k)= 1001

c= 0111 ⊕ 1001 = 1110

p= 1110 ⊕ 1001 = 0111

Limitations:

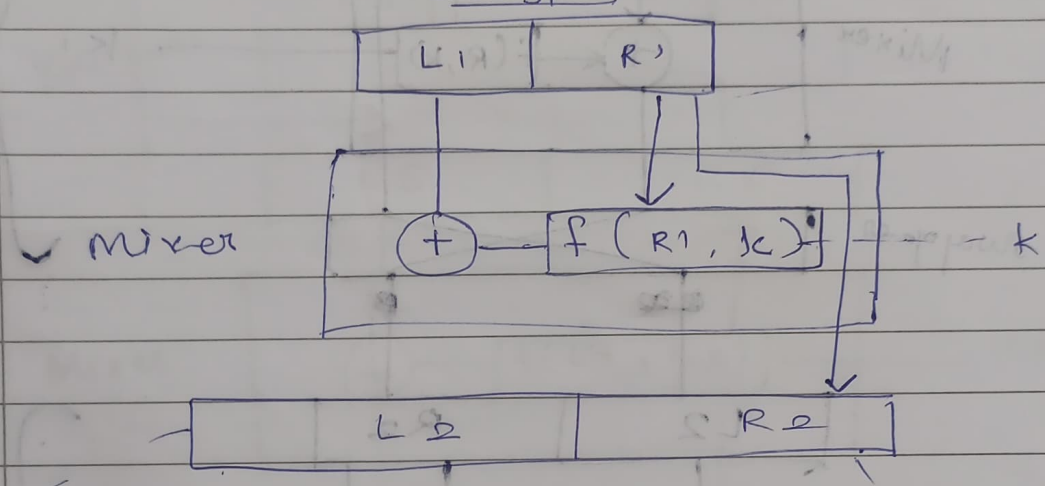
In the first draft of feister cipher Tech. is:

1. Function is applied on key only.

Second Draft of Feistel Cipher Tech.

In second draft of feistel Cipher Tech is function is applied on key as well as data.

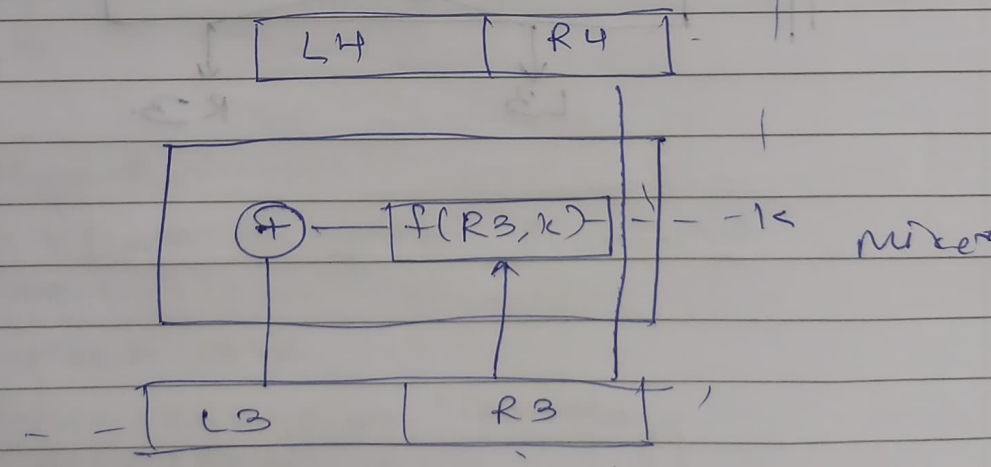
Encryption



$L_2 = L_1 \oplus f(R_1, k)$

$R_2 = R_1$

Decryption:

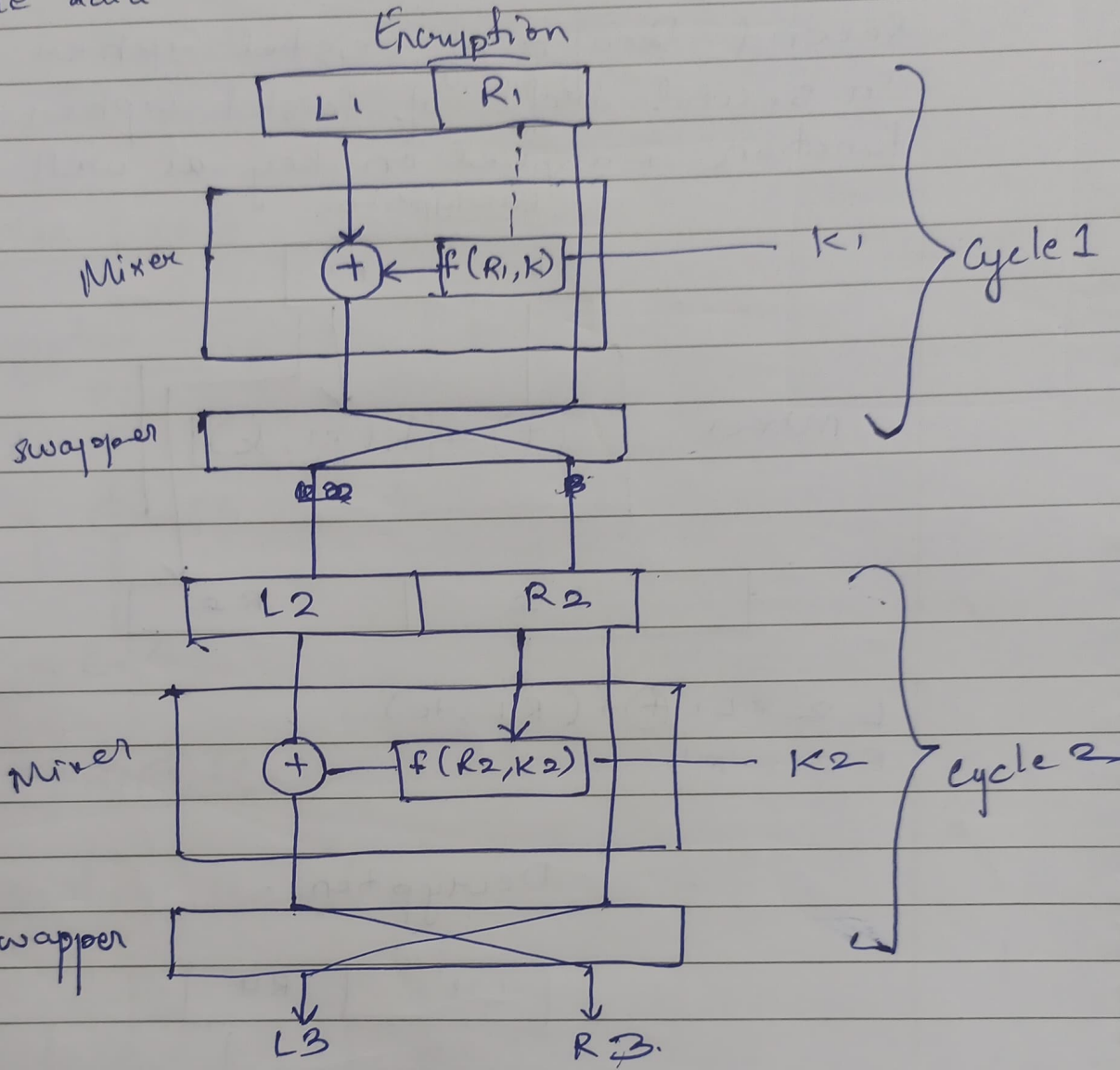


$L_4 = L_3 \oplus f(R_3, k)$

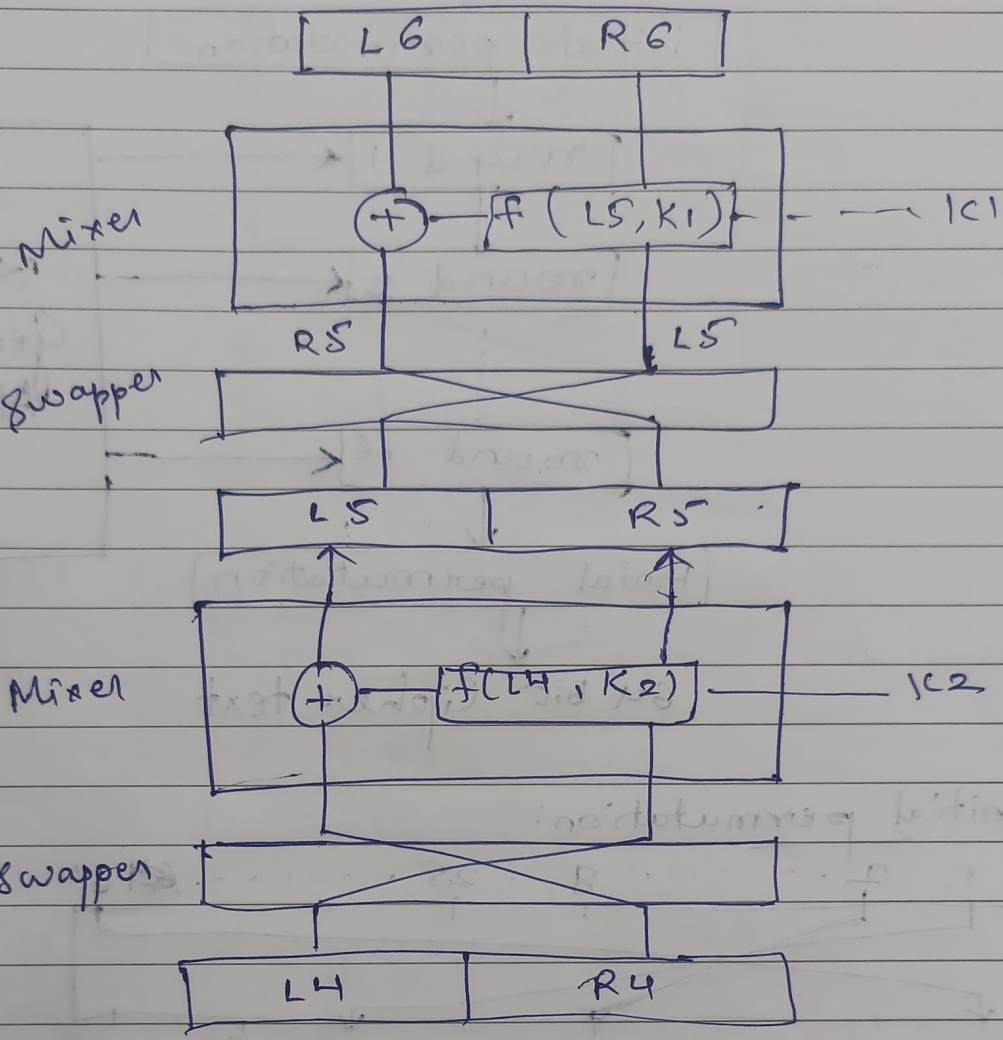
$R_4 = R_3$

Final Draft of Feistel Cipher

1. Increasing No. of Round.
2. Performing operation on left hand and Right hand side data.

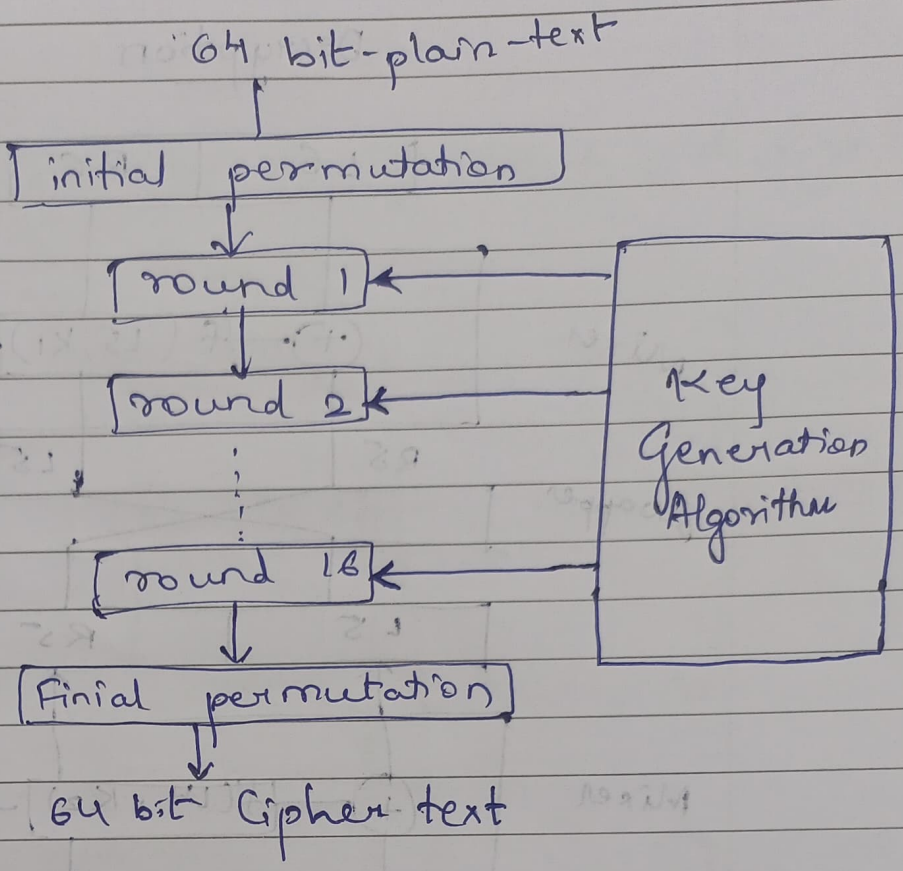


Decryption

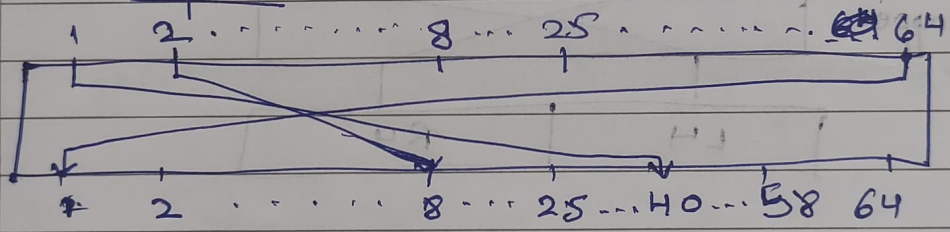


DES algorithm is based on fiesel cipher working principle

* DES Algorithm
  - DES → Data Encryption standards.
  - NIST →
  - DES - March 1975
  - Symmetric Encryption Technology.
  - 16 cycle / 16 - Rounds.
  - 16 keys
  - Brute force attack.
  - S-box - hidden trapdoor.

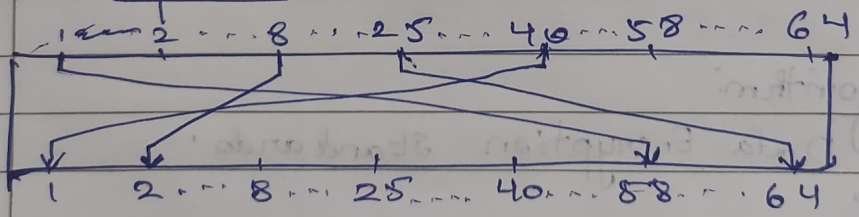


1] Initial permutation:



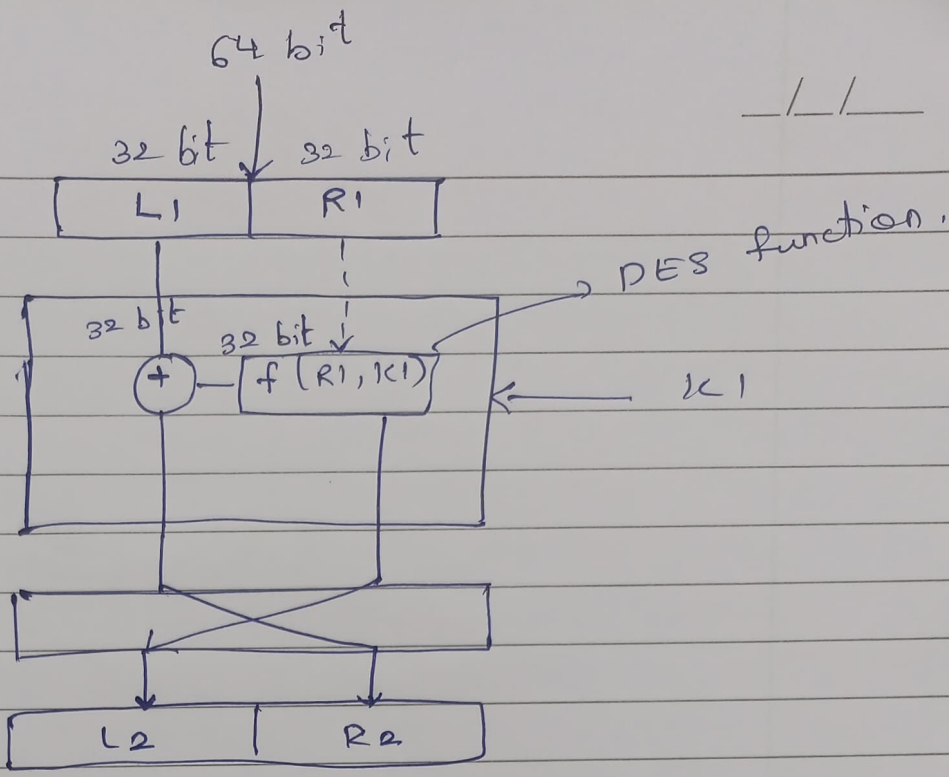
1 – 40
2 – 8
64 → 1

2] Final permutation:



1 – 58
8 – 2
25 – 64
40 – 1

3] Single cycle operation / Single Round operation:



DES function: